LONG HAUL NETWORK

LORAL DEFENSE SYSTEMS-AKRON
1210 MASSILLON ROAD
AKRON, OHIO 44315

1 November 1992

Document No. ALO1192-001

CRDL A002

Prepared for:
Air Force Human Resources Laboratory
Williams Air Force Base, AZ 85224

LORAL
Defense Systems - Akron

ADST SUBCONTRACT # E-91-108
MULTIRAD NETWORK

GLOSSARY OF TERMS

AIS	Automated Information System
AFB	Air Force Base
AIT	Air Intercept Trainer
ATES	Automated Threat Engagement System
AWACS, AWCS	Airborne Wide Area Command System
CET	Combat Engagement Trainer
COMSEC	Communications Security
CSO	Cognizant Security Office
DIS	Distributed Interactive Simulation
DL	Data Logger
GCI	Ground Controlled Intercept
IFF	Identification Friend or Foe
ISS	Information Systems Security
LHN	Long Haul Network
MDRC	McDonnell Douglas Reconfigurable Cockpit
MULTIRAD	Multiship Training Research and Development
NIU	Network Interface Device
NSA	National Security Administration
PVD	Plan View Display
SIMNET	Simulation Network
T1	A specific telephone trunk line specification
TED	Trunk Encryption Device
TRUE	Training Utility Evaluation
WPAFB	Wright Patterson AFB, OH

Statement A per telecon Col. Lynn Carroll
A/L Williams AFB, AZ 85224

NWW 12/12/94

TABLE OF CONTENTS

1.0 INTRODUCTION

The MULTIRAD complex at Williams AFB, AZ houses a GCI trainer, on Air Intercept Trainer (AIT) several pilot training devices, an Automated Threat Engagement System (ATES) and an Instructional Support System (ISS) all within a TEMPEST facility. Thus, integrated training exercises can be performed, controlled and monitored in a dedicated security environment. The next two stages of MULTIRAD development are the interim and the advanced MULTIRAD. Interim MULTIRAD with long haul network (LHN) and extensions of SIMNET protocol will be used for the training utility evaluation (TRUE). An extension of distributed interactive simulation (DIS) protocol will be introduced for advanced MULTIRAD.

2.0 OBJECTIVE

This plan provides security rationale and requirements for extension of the MULTIRAD development program into multi-site exercises over a LHN using DIS protocol.

3.0 APPROACH

3.1 Description of Plan

The plan is the result of a review of the documents listed in paragraph 3.2 as well as discussions and analysis of the security of data within an automated information system and AIS networks as they apply to the MULTIRAD program. This work was performed in October and November of 1991 at Loral Defense Systems - Akron, Ohio.

3.2 Applicable Documents

1ST-PD-90-2 (revised). Miliary Standard (draft) Protocol Data Units for Entity Information and Entity Interaction in a Distributed Interactive Simulation, September 20, 1991

Draft 19 Sep 91 Lot I MULTIRAD Network Research and Development, Section C with Appendices A and B

Bolt, Beranek, and Newman Systems and Technologies for the United States Air Force Armstrong Laboratories, Draft--Interim MULTIRAD Network Design Specification, June 25, 1991

Bolt, Beranek, and Newman Systems and Technologies for the United States Air Force Armstrong Laboratories, Network Interface Unit Detailed Design Specification, June 25, 1991

NSA Information Systems Security, Products and Services Catalogue July, 1991

DoD 5220.22-M Industrial Security Manual for Safeguarding Classified Information January, 1991. Chapter 8 "Automated Information Systems"

NCSC-TG-002, Version 1 Trusted Product Evaluations, A Guide for Vendors 22 June 1990

Specification NSA No. 89-5 Performance and Interface Specification for TSEC/KG-194, Trunk Encryption Device 18 January 1989

Cooper, James Arlin Computer and Communications Security, Strategies for the 90's McGraw Hill, 1989

NCSC-TG-005, Version 1 Trusted Network Interpretation, 31 July 1987

DoD 5200.28-STD Department of Defense Trusted System Computer System Evaluation Criteria December 1985

CSC-STD-004-85 Technical Rationale Behind CSC-STD-003-85 Computer Security Requirements

4.0 ANALYSIS

4.1 SECURITY RATIONALE

4.1.1. Classification of LHN data

Simulations within the MULTIRAD environment are simulations of real world classified systems. Emission parameters, missile parameters, stealth characteristics, and IFF doctrines, combined with position and event data, can yield overall weapon system effectiveness. The classification of overall weapon system effectiveness has always been the bottom line when determining security levels for Air Force weapon systems. Individual subsystem characteristics alone may be considered UNCLASSIFIED or CONFIDENTIAL but the of overall system weapon effectiveness usually requires a classification of SECRET.

If positional data is transferred without the accompanying appearance and event data, an exercise may still be considered SECRET. Since any of the weapon systems in a MULTIRAD exercise may be operated using operational doctrine and tactical expertise, it is likely that the compilation of positional data being passed between the systems on the MULTIRAD network will be rendered SECRET unless tactical maneuvers are forbidden and prevented. A mission rehearsal exercise, which uses specific locations, could upgrade the positions of weapon systems themselves to TOP SECRET.

In order to provide an effective weapon system, any LHN must be capable of transmitting TOP SECRET data between multiple sites. In order to do that, some type of encryption must be introduced.

4.1.2. The interim and advanced MULTIRAD network exercises must operate in a dedicated security environment.

Paragraph 8-206 of the Industrial Security Manual, DoD 5220.22-M, January 1991 states, ". . . On January 1, 1992, all AIS's [automated information systems] approved to process classified information in other than the dedicated mode will be required to meet the C2, or higher, level of trust criteria specified in DoD 5200.28-STD. . . . In the dedicated security mode trusted systems are not required. . . .".[1] "Dedicated" means that all users that have access to the data on a system must have a need-to-know and a security clearance at least as high as the highest level of the data available through that access route.

4.1 SECURITY RATIONALE (cont')

4.1.2 (Cont'd)
If a lower clearance individual or multiple needs-to know are given access to any of the data within the MULTIRAD system, the system is no longer considered dedicated. After January, 1992 the requirement to assure the integrity of classified portions of the system mandates that a C2 or higher trusted system approval must be obtained for each and every AIS device in the MULTIRAD system and for each and every AIS device at the remote sites as well. The approval process is an unknown but for the MULTIRAD operating requirements it does not appear to be a viable approach for the interim MULTIRAD development. In the future this option may provide a workable solution using the advanced MULTIRAD DIS protocol and should be examined again.

To alleviate security risks the interim MULTIRAD network environment must satisfy the dedicated system criteria. The sites in a MULTIRAD exercise must all operate at the same clearance level with the same need-to-know when the LHN links are activated. Also, data that flows between sites must be encrypted before it leaves controlled security boundaries at each site. If this approach is taken now, MULTIRAD can prove to be useful to those sites which have compatible security levels. Future development, when the proper C2 approvals have been obtained, can then attempt to upgrade the dedicated security environment to a system high security environment for the network to allow multiple need-to-know exercises limited access to the network. The sites must remain locally dedicated, however, because of their local networks.

4.1.3. The security for the MULTIRAD LHN should be administered and controlled from a centralized facility.

The MULTIRAD facility at Williams AFB, AZ contains the monitoring, auditing, logging and control equipment needed to administer security on the MULTIRAD LHN. It has been designed to be the hub of the MULTIRAD system. Using a central network security controller and star topology [2] (MULTIRAD facility at the center, remote sites at the points of the star) will simplify the network security process by reducing the number of security interfaces on the network to three. The central controller can then directly distribute the keying parameters to the remote sites and establish common procedures for access, identification and authentication. This also makes the security auditing process more manageable.

It should be noted that this means that the remote sites will have to include the central site administrator if they are to network with each other. Since over 80% of the entities in the proposed MULTIRAD network are located at Williams, this should be a workable solution.

Whether one exercise or multiple exercises are accessing the network, the central network security controller at Williams will still be authenticating, auditing and monitoring every exercise.

4.2 SECURITY REQUIREMENTS FOR THE LHN

A star network topology was chosen for its security advantages. The central network security manager has access to, and positive control of, all the interfaces and all the data transferred across the network. Data which is to be transmitted between sites must be encrypted to the B1 level before it leaves the protection of the security environment at each site. This data must be treated as SECRET or in some cases TOP SECRET. In all, 6 encryption devices will be required: Three at Williams and one at each of the remote sites. (See Figure 1 MULTIRAD NETWORK)

With multiple voice channels and assignment of a 2 Hz update rate to the 3K to 10K bit DIS entity packets the 69 entity network must be able to pass at least 1.5 Mbits per second. There are approved devices which satisfy such a bandwidth. Encryption devices and the three encrypted trunk lines must be able to handle the volume of data required to support the eventual DIS protocol for the 69 entities proposed. For example, the capabilities of TSEC/KG-194, -194A encryption devices interfacing with T1 trunk lines are specified to operate 1.544 Mbits per second.[3] The KG-194, -194A can protect ". . . all classifications of digital traffic."[3] If other bandwidths are desired other approved encryption devices are available. [3]

The central network security manager will establish network policy and control mechanisms. He must verify or approve:

1. The security level at each site. All three sites must have a security level at least as high as the highest level of the data in the system.

2. The trunk line penetration of the security shield at each site.

3. The protection mechanisms at each site for securing the encryption devices which contain valid keys. The devices are unclassified when the keys are cleared out.

4. The LHN start up, authentication and access procedures.

5. The LHN sign-off and shut down procedures.

6. The audit techniques which are selected to monitor the access to, and use of, the LHN.

5.0 CONCLUSIONS

1. To meet the requirements for security of TRUE, three encrypted duplex channels must be established, one from Williams to each of the three remote sites. (See Figure 1 MULTIRAD NETWORK)

2. Extended MULTIRAD exercises must be conducted in a dedicated security environment (i.e. all sites must be cleared to the same security level in order to obtain access to the data on the network).

3. The advanced MULTIRAD LHN exercises will still require that all devices at a given site be operated within a locally dedicated security environment.

4. The security for the MULTIRAD LHN should be administered and controlled from the MULTIRAD facility at Williams AFB, AZ.

6.0 REFERENCED DOCUMENTS

[1] DoD 5220.22-M Industrial Security Manual for Safeguarding Classified Information January, 1991. Chapter 8 "Automated Information Systems"

[2] Cooper, James Arlin Computer and Communications Security, Strategies for the 90's McGraw Hill, 1989

[3] NSA Information Systems Security, Products and Services Catalogue July, 1991

FIGURE 1

MULTIRAD NETWORK